Cryptography and Security of Digital Devices

Notes on abstract algebra and modular arithmetic

Euclid's Algorithm, Polynomial rings and Polynomial fields

Gerardo Pelosi

Exam Code 090959 – A.Y. 2013-2014, Semester 2
Politecnico di Milano

1 Euclid's algorithm

On the integral domains $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{F}[X], +, \cdot)$ it is possible to define the common notion of order relation (between integer or polynomials) and the common notion of division between elements, for such a reason they are also called *Euclidean Domains.*

Definition 1.1 (Greatest Common divisor)**.** *Let* $\mathbf{D}$ *be either* $(\mathbb{Z}, +, \cdot)$ *or* $(\mathbb{F}[X], +, \cdot)$*. The* Greatest Common Divisor *between any two elements* $a, b \in D$*,* $\gcd(a, b)$*, is defined as the element* $d \in \mathbf{D}$ *such that* $d|a$*,* $d|b$ *and* $\forall y \in D$*,* $y|a \wedge y|b \Rightarrow y|d$*.*

Informally, we recall that, given $a, b \in \mathbf{D}$ if $d \in \mathbf{D}$ is their gcd, then d divides also every linear combination of them, that is: $d|(\xi \cdot a + \eta \cdot b)$ with $\xi, \eta \in \mathbf{D}$.

Considering any two elements $a, b \in \mathbf{D}$, it is possible to prove, together with the existence of a gcd d also the existence of at least a pair of elements $x_a, x_b \in \mathbf{D}$ such that

$$d = x_a a + x_b b$$

This result will allow us to compute the multiplicative inverse in a finite field.

Lemma 1.1. *Given two elements* $a, b \in \mathbf{D}$*, with* $a \geq b > 0$*; if* $\mathbf{D}$ *is either* $(\mathbb{Z}, +, \cdot)$ *or* $(\mathbb{F}[X], +, \cdot)$ *we can define the concept of quotient, that is* $q = \lfloor a/b \rfloor$*. Once the definition of quotient is given, we define as remainder* $r = a \bmod b = a - qb \in \{0, 1, 2 \ldots, b-1\}$*. Assumed these premises, the following equality holds:*

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

In case one of the operands is zero we assume that $\gcd(a, 0) = a$*,* $\forall\, a \in \mathbf{D}$

Employing the previous lemma, it is possible to write down the following relations:

$$\begin{array}{ll}
a > b > 0 & d = \gcd(a, b) \\
r_0 = a & \\
r_1 = b & d = \gcd(r_0, r_1) \\
r_2 = r_0 \bmod r_1 = r_0 - \lfloor r_0/r_1 \rfloor r_1;\ \ 0 \leq r_2 < r_1 & d = \gcd(r_1, r_2) \\
r_3 = r_1 \bmod r_2 = r_1 - \lfloor r_1/r_2 \rfloor r_2;\ \ 0 \leq r_3 < r_2 & d = \gcd(r_2, r_3) \\
r_4 = r_2 \bmod r_3 = r_2 - \lfloor r_2/r_3 \rfloor r_3;\ \ 0 \leq r_4 < r_3 & d = \gcd(r_3, r_4) \\
\ldots & \ldots \\
r_n = r_{n-2} \bmod r_{n-1} = r_{n-2} - \lfloor r_{n-1}/r_{n-2} \rfloor r_{n-2};\ \ r_n = 0 & d = \gcd(r_{n-1}, 0)
\end{array}$$

for a given integer n the following hold:

$$d = \gcd(a, b) = r_{n-1}$$

Rewrite now all the steps as a linear combination of a, b only:

$$
\begin{aligned}
&a > b > 0 \\
&r_0 = 1 \cdot a + 0 \cdot b \\
&r_1 = 0 \cdot a + 1 \cdot b \\
&r_2 = r_0 \bmod r_1 = (1a + 0b) - \lfloor \tfrac{r_0}{r_1} \rfloor (0a + 1b) = (\xi_2 a + \eta_2 b);\ 0 \leq r_2 < r_1 \\
&r_3 = r_1 \bmod r_2 = (0a + 1b) - \lfloor \tfrac{r_1}{r_2} \rfloor (\xi_2 a + \eta_2 b) = (\xi_3 a + \eta_3 b);\ 0 \leq r_3 < r_2 \\
&r_4 = r_2 \bmod r_3 = (\xi_2 a + \eta_2 b) - \lfloor \tfrac{r_2}{r_3} \rfloor (\xi_2 a + \eta_2 b) = (\xi_4 a + \eta_4 b);\ 0 \leq r_4 < r_3 \\
&\dots \\
&r_{n-1} = r_{n-3} \bmod r_{n-2} = (\xi_{n-3} a + \eta_{n-3} b) - \lfloor \tfrac{r_{n-3}}{r_{n-2}} \rfloor (\xi_{n-2} a + \eta_{n-2} b) = \\
&\qquad = (\xi_{n-1} a + \eta_{n-1} b);\ 0 \leq r_{n-1} < r_{r-2} \\
&r_n = r_{n-2} \bmod r_{n-1} = (\xi_{n-2} a + \eta_{n-2} b) - \lfloor \tfrac{r_{n-3}}{r_{n-2}} \rfloor (\xi_{n-1} a + \eta_{n-1} b) = \\
&\quad = (\xi_n a + \eta_n b);\ r_n = 0
\end{aligned}
$$

thus,

$$d = r_{n-1} = \xi_{n-1} a + \eta_{n-1} b;\ \ \xi, \eta \in D$$

Formalizing properly the previous derivations, we obtain the Euclid's algorithm for the computation of the greatest common divisor.

Algorithm 1.1: Extended Euclid Algorithm

Input: $a, b \in D$
Output: $d = \xi \cdot a + \eta \cdot b,\ \xi, \eta \in \mathbf{D}$

```
1  begin
2      u ← (a, 1, 0) // array with three elements:  u[0], u[1], u[2]
3      v ← (b, 0, 1)
4      repeat
5          w ← u − ⌊u[0]/v[0]⌋ · v
6          u ← v
7          v ← w
8      until (w[0] = 0)
9      d ← u[0], ξ ← u[1], η ← u[2]
10     return (d, ξ, η)
```

The algorithm can be re-written to make use of only subtraction operations with a computational complexity linear in the bit-length of the input operands and equal to $\mathcal{O}\big(2\ \log(\max\{a, b\})\big)$ addition/subtraction operations (Refer to Chap. 14, Menezes et al. *Handbook of Applied Cryptography*, CRC Press)

Example 1.1. *Let* $D =< Z, +, \cdot >$

$d = \gcd(11, 5) = 11\xi + 5\eta$*;*

$\underline{u} \leftarrow (11, 1, 0)$*;*
$\underline{v} \leftarrow (5, 0, 1)$*;*

$q = \lfloor \frac{11}{5} \rfloor = 2$, $\underline{w} \leftarrow (11 - 2 \cdot 5, 1 - 0 \cdot 2, 0 - 1 \cdot 2) = (1, 1, -2)$*;*
$\underline{u} \leftarrow (5, 0, 1)$*;*
$\underline{v} \leftarrow (1, 1, -2)$*;*

$q = \lfloor \frac{5}{1} \rfloor = 5$, $\underline{w} \leftarrow (5 - 1 \cdot 5, 0 - 1 \cdot 5, 1 - (-2) \cdot 5) = (0, -5, 11)$*;*
$\underline{u} \leftarrow (1, 1, -2)$*;*
$\underline{v} \leftarrow (0, -5, 11)$*;*

$d = 1$*;* $\xi = 1$*;* $\eta = -2$*.*

in fact: $1 = 1 \cdot 11 + (-2) \cdot 5$*.*

2 The Groups $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n^*, \cdot)$

These groups are particularly useful in cryptography. We have seen that $(\mathbb{Z}_n, +)$ can be easily shown to be a cyclic group. The inverse of any element a is given by its opposite $-a \equiv |\mathbb{Z}_n| - a$.

Considering $(\mathbb{Z}_n^*, \cdot)$, the support $\mathbb{Z}_n^*$ is defined to include the representatives of the equivalence classes modulo n which are smaller than n and no common factor with n except for the neutral element 1: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \,\text{s.t.}\, gcd(n, a) = 1\}$, therefore the cardinality of such group is given by the Totient function of n: $|(\mathbb{Z}_n^*, \cdot)| = \varphi(n)$. Given any two elements $a, b \in \mathbb{Z}_n^*$, the application of the group law $a \cdot b$ computes the remainder of the integer division between the integer product $a \times b$ and the divisor n.

Example 2.1. $(\mathbb{Z}_{15}^*, \cdot)$ *contains the representatives of the classes modulo* 15*. In particular,* $(\mathbb{Z}_{15}^*, \cdot) = \{1, 2, 4, 7, 8, 11, 13, 14\}$*. The cardinality of* $\mathbb{Z}_{15}^*$ *is thus the number of positive integers, coprime with* 15 *and smaller than* 15*, i.e.* $\varphi(15) = \varphi(3 \times 5) = (3^1 - 3^0) \times (5^1 - 5^0) = 2 \times 4 = 8$*.*

It is easy to demonstrate that $(\mathbb{Z}_n^*, \cdot)$ is a commutative group with neutral element 1, through showing a constructive way to compute the inverse of any element.

Since for each element $x \in \mathbb{Z}_n^*$ must be true that $\gcd(x, n) = 1$ (i.e. x and n are coprime), we can consider x and n as elements of the Euclidean ring $\mathbb{Z}$ and apply Euclid's algorithm:

$$\gcd(n, x) = 1 \;\Rightarrow \exists\, \xi, \eta \in \mathbb{Z} :\; \xi\, n + \eta\, x = 1$$

Thus, considering both sides modulo n, we obtain that:

$$x^{-1} \mod n \equiv \eta \mod n, \quad x^{-1} = (\eta \mod n) \in \mathbb{Z}_n^*$$

Example 2.2. *In* $(\mathbb{Z}_{15}^*, \cdot)$ *consider* $x = 7$ *then*

$$gcd(15, 7) = 1 \Rightarrow (1) \times 15 + (-2) \times 7 = 1$$

$$x^{-1} = (-2 \bmod 15) = 13 \in \mathbb{Z}_{15}^*$$

Therefore $(\mathbb{Z}_n^*, \cdot)$ is a commutative group in general. For completeness' sake we report the following:

Theorem 2.1. *The group* $(\mathbb{Z}_n^*, \cdot)$ *is cyclic if and only if* n=$1, 2, 4, n$=p^k, n=$2p^k$ *where* $k \geq 1$ *and* $p \geq 3$ *is a prime integer.*

For instance, $(\mathbb{Z}_p^*, \cdot)$ is cyclic, it contains exactly $p-1$ elements $(\mathbb{Z}_p \backslash \{0\})$ for every possible prime p, and $\varphi(p-1)$ generators. Note that if g is a generator, the elements g^h with order $p-1$ (generators) will be

$$\varphi(p-1) = |\{1 \leq h < p-1 : \gcd(p-1, h) = 1\}|$$

Proposition 2.1 (Numerical Finite fields)**.** *The finite group* $(\mathbb{Z}_p^*, \cdot)$ *is cyclic and also the finite group* $(\mathbb{Z}_p, +)$ *is cyclic therefore, the structure* $(\mathbb{Z}_p, +, \cdot)$ *is a finite field.*
The field $(\mathbb{Z}_p, +, \cdot)$ *is also denoted as* $\mathbb{Z}/(p)$ *or* $\mathbb{Z}/p\mathbb{Z}$*.*

Proving that $\mathbb{Z}_p$ is a field can be done through a direct validation that all the elements except 0 has a multiplicative inverse. Indeed, given $r \in \mathbb{Z}_p$, being $\gcd(p, r) = 1$ then there exist two integers ξ, η such that $1 = \xi p + \eta r \Rightarrow r^{-1} \equiv \eta \bmod p \; \forall \, r \in \mathbb{Z}_p$

2.1 Computing inverses in $(\mathbb{Z}_n^*, \cdot)$

The inverses in $(\mathbb{Z}_n^*, \cdot)$ with any $n \geq 2$ can be computed in two distinct ways:

- either through the extended Euclid algorithm
- or via the properties of the groups

In particular, since $(\mathbb{Z}_n^*, \cdot)$ is a finite group with order $|\mathbb{Z}_n^*| = \varphi(n)$, each one of its elements will have an order dividing $\varphi(n)$. Consequently, it is true that:

$$x \in \mathbb{Z}_n^*, \; x^{\varphi(n)} \equiv 1 \mod n, \quad \text{(relation known as Euler's theorem)}$$

Therefore

$$x \in \mathbb{Z}_n^*, \; x^{\varphi(n)} \equiv 1 \mod n \; \Rightarrow \; x^{-1} \equiv x^{\varphi(n)-1} \mod n$$

An efficient method for computing a modular exponentiation is essential. The most naive way to compute a^n is to do $n-1$ multiplications of the element a with itself. In practical applications most choices of n are large enough that it would be infeasible to compute a^n using $n-1$ successive multiplications by a. There are two ways to reduce the time required to do an exponentiation. One way is to decrease the time to multiply two elements in the group; the other is to reduce the number of multiplications used to compute a^n. Ideally, one would do both. We now consider the general techniques for exponentiation.

The problem can be re-formulated as follows: Given $a, n \in \mathbb{N}$, we want to compute the integer $c = a^n$ through employing a number of multiplications

much smaller than n.
Let t be the number of binary digits necessary to encode the value n, that is:

$$t = \lceil \lg_2 n \rceil,\ n = (n_{t-1}, \ldots, n_1, n_0) \text{ with } n_i \in \{0,1\},\ i \in \{0,1,\ldots,t-1\}$$

we can write that:

$$c = a^n = a^{\sum_{j=0}^{t-1} n_j 2^j} = a^{n_{t-1}2^{t-1} + n_{t-2}2^{t-2} + \ldots + n_1 2^1 + n_0} \tag{1}$$

Depending on the way we read (interpret) the last member of the above equality chain, two different exponentiation algorithms (known as *Square and Multiply(S&M) algorithms*) can be formulated.

2.1.1 Square and Multiply - Left to Right

Assuming to scan the bits of the exponent n in the equation (1) from left to right, the following equality holds:

$$c = a^n = ((\cdots((a^{n_{t-1}})^2 \cdot a^{n_{t-2}})^2 \cdots)^2 \cdot a^{n_1})^2 \cdot a^{n_0}$$

Example 2.3. *Given the following operation $c = 5^6$; we have that $a = 5$, $t = 3$, $n = 6_{\text{decimal}} = \langle 110 \rangle_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$, then:*

$$c = 5^{\langle 110 \rangle_2} = ((5^1)^2 \cdot 5^1)^2 \cdot 5^0 = (5^2 \cdot 5)^2 = 15625.$$

The computational cost of this method, expressed in terms of squarings and multiplications needed to compute the final result, is (on average): $t-1$ squarings, plus $\frac{1}{2}(t-1)$ multiplications, with $t = \lceil \lg_2 n \rceil$.

Algorithm 2.1: S&M Left to Right

Input: a, n, $t = \lceil \lg_2 n \rceil$, $n = (n_{t-1}, \ldots, n_1, n_0), n \geq 0$
Output: $c = a^n$

```
1 begin
2     if n = 0 then
3         return 1
4     c ← a
5     for i ← t − 2 down-to 0 do
6         c ← c^2
7         if n_i = 1 then
8             c ← c · a
9     return c
```

2.1.2 Square and Multiply - Right to Left

Assuming to scan the bits of the exponent n in the equation (1) from right to left, the following equality holds:

$$c = a^n = (a^{2^0})^{n_0} \cdot (a^{2^1})^{n_1} \cdot (a^{2^2})^{n_2} \cdots (a^{2^{t-1}})^{n_{t-1}}$$

Example 2.4. *Given the following operation $c = 5^6$; we have that $a = 5$, $t = 3$, $n = 6 = \langle 110 \rangle_2 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$, then:*

$$c = 5^{110_2} = (5^{2^0})^0 \cdot (5^{2^1})^1 \cdot (5^{2^2})^1 = (5 \cdot 5^2 \cdot 5^4) = 15625.$$

Note that the factor a^{2^j} can be computed re-using the previous factor and employing only one squaring operation: $\left(a^{2^{j-1}}\right)^2$

Analogously to the previous method, the computational cost of this technique, expressed in terms of squarings and multiplications needed to compute the final result, is (on average): $t-1$ squarings, plus $\frac{1}{2}(t-1)$ multiplications, with $t = \lceil \lg_2 n \rceil$.

Algorithm 2.2: S&M Right to Left

Input: a, n, $t = \lceil \lg_2 n \rceil$, $n = (n_{t-1}, \ldots, n_1, n_0), n \geq 0$
Output: $c = a^n$

```
1  begin
2      if n = 0 then
3          return 1
4      b ← a
5      if n_0 = 1 then
6          c ← a
7      else
8          c ← 1
9      for i ← 1 to t − 1 do
10         b ← b^2
11         if n_i = 1 then
12             c ← c · b
13     return c
```

A generalization of the S&M algorithms consists of processing more than one exponent bit at time (which is equivalent to encode the exponent in a numerical base $b = 2^k$ for some k), to trade-off the storage needed for some pre-computation with the efficiency of the squaring and multiplication operations. For example:

Algorithm 2.3: Window method

Input: a, n, $t = \lceil \lg_b n \rceil$, $n = (n_{t-1}, \ldots, n_1, n_0)$, $n \geq 0$, $b = 2^k$
Output: $c = a^n$

```
1  begin
2      if n = 0 then
3          return 1
4      g_0 ← 1
5      for i ← 1 to 2^k − 1 do
6          g_i ← g_{i−1} · a
7      c ← g_{n_{t−1}}
8      for i ← t − 2 down-to 0 do
9          c ← c^{2^k}
10         if n_i ≠ 0 then
11             c ← c · g_{n_i}
12     return c
```

3 Chinese remainder theorem (CRT)

Due to its usefulness in implementing efficient cryptosystems, we recall the following very old piece of mathematics, which dates back at least 2000 years. We shall use the CRT in a few places, for example to improve the performance of the decryption operation of RSA and in a number of other protocols.

Theorem 3.1 (Chinese Remainder Theorem)**.**
Let $n_1, \ldots, n_k$ be k positive integers pairwise coprime, and let $x_1, \ldots, x_k$ be k elements of $\mathbb{Z}$. The following system of modular congruences

$$\begin{cases} X \equiv x_1 \pmod{n_1} \\ X \equiv x_2 \pmod{n_2} \\ X \equiv x_3 \pmod{n_3} \\ \cdots \\ X \equiv x_k \pmod{n_k} \end{cases}$$

has a unique solution $\overline{X}$ such that $0 \leq \overline{X} < N$, with $N = \prod_{i=1}^{k} n_i$.

Theorem 3.2 (Chinese Remainder Theorem - alternate definition)**.**
Let X, n be positive integers, such that:

$$N = \prod_{i=1}^{k} n_i = n_1 \cdot n_2 \cdot n_3 \cdot \cdots \cdot n_k$$
$$\forall i, j \in \{1, \ldots, k\}, i \neq j \quad gcd(n_i, n_j) = 1$$

The relation

$$X \mapsto (x_1, x_2, \ldots, x_n)$$
$$\text{with} \quad X \equiv x_i \bmod n_i \quad (0 \leq x_i < n_i)$$

is bijective.

Proof. (Sketch)

- Given X and a k-uple of integers, $(n_1, n_2, \ldots, n_k)$ pairwise coprime, proving that there is only one k-uple $\{x_1, x_2, \ldots, x_k\}$, with $0 \leq x_i < n_i$, fitting the relation is trivial: it is sufficient to consider the k-uple ($X \bmod n_1, X \bmod n_2, \ldots, X \bmod n_k$) for the relation to hold.
- We now prove that given a k-uple $(x_1, x_2, \ldots, x_k)$, $0 \leq x_i < n_i$, such that $\forall i \neq j \ \gcd(n_i, n_j) = 1$, it is possible to associate only one positive integer $X \bmod N$ with $N = \prod_{i=1}^{k} n_i$.

  In order to do so, let M_i and M_i' be: $M_i = \frac{N}{n_i}$ and $M_i' = M_i^{-1} \bmod n_i$, respectively. Note that it is always possible to compute M_i' since all the n_i values are coprime by construction with M_i.
  We note that:

  $$M_i \cdot M_i' \equiv 1 \bmod n_i \qquad \forall i \in \{1, 2, \ldots, k\}$$
  $$M_i \cdot M_i' \equiv 0 \bmod n_j \qquad \forall i \in \{1, 2, \ldots, k\}, j \neq i$$

  The first observation is rather trivial as M_i e M_i' are one the inverse of the other by construction.

The second observation employs the fact that, by construction, M_i is a multiple of all the values n_j except for n_i.

It is thus easy to verify that the positive integer number X, $0 \leq X < N$ defined as:

$$X \triangleq \left(\sum_{i=1}^{k} M_i \cdot M_i' \cdot x_i \right) \bmod N \tag{2}$$

is the smallest positive integer bound to the tuple $(x_1, x_2, \ldots, x_k)$, where $\forall i \, X \equiv_{n_i} x_i$. In fact, all the elements of the sum are equal to zero mod n_i except for the i-th one.

□

4 Polynomial Rings

Given a field $(\mathbb{F}, +, \cdot)$, the set $\mathbb{F}[x] = \{a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \mid a_i \in \mathbb{F},\ n \geq 0\}$ of the polynomials with coefficients over $\mathbb{F}$ is an integral domain with respect to the usual sum and product of polynomials, called *polynomial ring in the unknown x over the field* $(\mathbb{F}, +, \cdot)$. Given two polynomials $f(x)$ and $g(x)$ with degrees n and $m \leq n$, respectively, we have that: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, g(x) = b_m x^m + b_{m-1}x^{n-1} + \ldots + b_1 x + b_0$

$$f(x)+g(x) = a_n x^n + \ldots + a_{m+1}x^{m+1} + (a_m + b_m)x^m + \ldots + (a_1 + b_1)x + (a_0 + b_0)$$

$$f(x) \cdot g(x) = (a_n \cdot b_m)x^{n+m} + \ldots + (\sum_{h+k=i,\ h,k\geq 0} a_h \cdot b_k)x^i + \ldots + (a_0 \cdot b_0)$$

The coefficient of the highest degree term of a polynomial $f(x) \in \mathbb{F}[x]$ is known as *leading coefficient*, and a polynomial having a leading coefficient equal to 1 is called *monic polynomial*.

Analogously to the ring $\langle \mathbb{Z}, +, \cdot \rangle$, it is possible to give a sorting notion among polynomials and a notions for division, quotient and reminder. These definitions are the same employed for polynomials with real ($\mathbb{R}$) coefficients, except that here the division between two coefficients $a, b \in \mathbb{F}$ must be computed as the multiplication of the first factor by the inverse of the second factor (i.e. $a \cdot b^{-1}$).

Proposition 4.1. *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, and $g(x) = b_m x^m + b_{m-1}x^{n-1} + \ldots + b_1 x + b_0$ be two polynomials in $\mathbb{F}[x]$, $g(x) \neq 0$, there exist two unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ and $0 \leq \text{degree}(r(x)) < \text{degree}(g(x))$.*

Proof. If $m > n$ then $q(x) = 0$ and $r(x) = f(x)$ are the only two polynomials that satisfy the requirements. In the non-trivial case $m \leq n$, the degree of $q(x)$ must be $n - m$ in order for the maximum degree term of $f(x)$ to be generated. Let $q(x) = q_{n-m}x^m + q_{n-m-1}x^{n-m-1} + \ldots + q_1 x + q_0$, $r(x) = r_{m-1}x^{m-1} + r_{m-2}x^{m-2} + \ldots + r_1 x + r_0$. If the equality $f(x) = g(x)q(x) + r(x)$ must hold then the coefficients of $q(x)$ and $r(x)$ should satisfy the following relations in $\mathbb{F}$:

$$\begin{aligned}
&b_m \cdot q_{n-m} = a_n \\
&b_m \cdot q_{n-m-1} + b_{m-1} \cdot q_{n-m} = a_{n-1} \\
&\ldots \\
&b_{m-1} \cdot q_0 + b_{m-2} \cdot q_1 + \ldots + b_0 \cdot q_{m-1} + r_{m-1} = a_{m-1} \\
&\ldots \\
&b_0 \cdot q_0 + r_0 = a_0
\end{aligned}$$

the first equation admits only one solution: $q_{n-m} = b_m^{-1}a_n$. Through replacing this value in the 2nd equation we obtain a unique value for $q_{n-m-1} = b_m^{-1}(a_{n-1} - b_{m-1} \cdot b_m^{-1}a_n)$. Repeating this kind of substitutions over the first $n-m$ equations, we can find all the coefficients of $q(x)$, while going through the remaining m equations, we derive the coefficients of $r(x)$. □

In the following the remainder $r(x)$ of the division between two polynomials $f(x)$ and $g(x)$ will be denoted as $f(x) \bmod g(x)$.

Definition 4.1 (Root of a polynomial)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{F}[x]$. The element $a \in \mathbb{F}$ is known as* root *of $f(x)$ if $a_n \cdot a^n + a_{n-1} \cdot a^{n-1} + \ldots + a_1 \cdot a + a_0 = 0$, where the operations $+, \cdot$ are now the ones of $(\mathbb{F}, +, \cdot)$.*

Theorem 4.1 (Ruffini's theorem)**.**
The polynomial $f(x) \in \mathbb{F}[x]$ has a root a if and only if $x - a$ divides $f(x)$.

Proof.

$\overset{\text{if part}}{\Rightarrow}$ $x - a$ divides $f(x)$ implies that $f(x) = g(x)(x - a)$, it is thus trivial to check that a is a root of $f(x)$.

$\overset{\text{only if part}}{\Leftarrow}$ Assume $f(x)$ has a root a, we thus know that $f(a) = 0$. Now, dividing $f(x)$ by $(x - a)$, we obtain that $f(x) = (x - a)g(x) + r(x)$, but, as the degree of the reminder is lower than the one of the divisor, and the divisor has degree 1, $r(x)$ is effectively an element of $\mathbb{F}$. Employing these results we obtain that $f(a) = (a - a)g(a) + r = 0$, from which $r = 0$ is derived, thus $(x - a)$ divides $f(x)$

□

Definition 4.2 (Root multiplicity)**.**
Let $a \in \mathbb{F}$ be a root of $f(x) \in \mathbb{F}[x]$. The root multiplicity of a is defined as the largest positive integer k such that $(x - a)^k$ divides $f(x)$, but $(x - a)^{k+1}$ does not.

It is possible to prove that $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ admits a as root with multiplicity ≥ 2 if $x - a$ divides also the formal derivative of $f(x)$: $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$

Definition 4.3 (Reducible and Irreducible Polynomials)**.**
A polynomial $f(x) \in \mathbb{F}[x]$ of degree n is defined **reducible** *in $\mathbb{F}$ if there exist two polynomials $g(x), h(x) \in \mathbb{F}[x]$ with $0 < \deg(g(x)) < n$ and $0 < \deg(h(x)) < n$ such that $f(x) = g(x)h(x)$.*
In case such polynomials do not exist $f(x)$ is defined as **irreducible** in $\mathbb{F}$.

We note that a polynomial over $\mathbb{F}[x]$ with degree lesser or equal to 3 is reducible if and only if it admits a root over $\mathbb{F}$. For instance, $f(x) = x^3 + 1 \in \mathbb{Z}_3[x]$ has a root $a = 2 \in \mathbb{Z}_3$, indeed $f(x) = (x^2 - x + 1)(x + 1) = (x + 1)^3 = (x - 2)^3$. Conversely, if a polynomial in $\mathbb{F}[x]$ has degree greater or equal to 4 it could be factored in irreducible terms, all with degree at least 2, thus resulting in having no factors with degree 1 (i.e. no roots over $\mathbb{F}$). For instance, $g(x) = x^4 + 2x^3 + 2x + 2 \in \mathbb{Z}_3$ does not have roots in $\mathbb{Z}_3$ as $g(0) \neq 0$, $g(1) \neq 0$, and $g(2) \neq 0$. However, it is easy to verify that $g(x)$ admits the two following irreducible factors: $g(x) = (x^2 + 1)(x^2 + 2x + 2)$.

Theorem 4.2 (Unique factorization)**.**
A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{F}[x]$ can be rewritten as a product of factors in the form: $f(x) = a_n g_1(x)\, g_2(x) \ldots g_r(x)$ where $r \leq n$ where all the $g_i(x)$ with $1 \leq i \leq r$ are monic and irreducible over $\mathbb{F}[x]$.
The aforementioned form is commonly called "factorization of a polynomial".

It is useful to note that the sum of the multiplicities of the roots of a polynomial over $\mathbb{F}$ is lesser or equal to its degree.
The equality holds if there are no factors with degree greater than 1 in the factorization of the polynomial.

Definition 4.4 (Greatest Common Divisor for Polynomials)**.**
Let $f(x), g(x)$ be two polynomials in $\mathbb{F}[x]$. The polynomial $d(x)$ which divides both $f(x)$ and $g(x)$, and such that any polynomial $h(x)$ that divides both $f(x)$ and $g(x)$ also divides $d(x)$ is defined to be the greatest common divisor *of $f(x)$ and $g(x)$ (denoted $\gcd(f(x), g(x))$).*

Note that: given $f(x), g(x) \in \mathbb{F}[x]$ (not equal to zero, simultaneously) if $d(x) = \gcd(f(x), g(x))$ then also $k\,d(x) = \gcd(f(x), g(x))$ for all $k \in \mathbb{F}$.
Among all the possible polynomials $k\,d(x)$, the monic polynomial is commonly assumed as the gcd (i.e., given any $k\,d(x)$, the $k^{-1}a^{-1}d(x)$ is assumed as gcd, where a is the leading coefficient of $d(x)$)
Through employing the Unique factorization theorem, the gcd of two polynomials can be obtained as the product of their common monic irreducible factors with minimal multiplicity. However, the factorization of a generic polynomial requires a costly algorithm thus, the Euclid's Algorithm is usually employed.

Example 4.1. *Consider $f(x), g(x) \in \mathbb{Z}_3[x]$ with $f(x) = x^2 - x - 1$, $g(x) = x + 1$*

$$d(x) = \gcd(f(x), g(x)) = \xi(x)f(x) + \eta(x)g(x)$$

$$\begin{cases} \underline{u} \leftarrow (x^2 - x - 1, 1, 0); \\ \underline{v} \leftarrow (x + 1, 0, 1); \end{cases}$$

$$\begin{cases} q = \lfloor \frac{x^2 - x - 2}{x+1} \rfloor = x - 2,\ \underline{w} \leftarrow (x^2 - x - 1 - (x+1)(x-2), 1, -(x-2)); \\ \underline{u} \leftarrow (x + 1, 0, 1); \\ \underline{v} \leftarrow (1, 1, -x + 2); \end{cases}$$

$$\begin{cases} q = \lfloor \frac{x+1}{1} \rfloor = x + 1,\ \underline{w} \leftarrow (x + 1 - (x+1), 0 - (x+1), 1 - (-x+2)(x+1)); \\ \underline{u} \leftarrow (1, 1, 2x + 2); \\ \underline{v} \leftarrow (0, 2x + 2, x^2 - x - 1); \end{cases}$$

$$d(x) = 1;\ \xi(x) = 1;\ \eta(x) = 2x + 2 \Rightarrow 1 = (1)f(x) + (2x + 2)g(x)$$

5 Polynomial Fields

Definition 5.1. *Let $\mathbb{F}$ be a field, and let $f(x) \in \mathbb{F}[x]$ be a fixed polynomial over $\mathbb{F}$. If $a(x), b(x) \in \mathbb{F}[x]$, then we say that $a(x)$ and $b(x)$ are congruent modulo $f(x)$, written*

$$a(x) \equiv b(x) (\mathrm{mod}\, f(x))$$

if $f(x)|(a(x) - b(x))$. The set $\{\, b(x) \in \mathbb{F}[x] \,\mathrm{s.t.}\, a(x) \equiv b(x) \bmod f(x) \,\}$, is called the congruence class of $a(x)$ (denoted by $[a(x)]$) and contains all polynomials with degree ≥ 0 and smaller than deg($f(x)$). The set of all congruence classes modulo $f(x)$ will be denoted by $\mathbb{F}[x]/(f(x))$.

Proposition 5.1. *Let $\mathbb{F}$ be a field, and let $f(x)$ be a nonzero polynomial in $\mathbb{F}[x]$. For any $a(x) \in \mathbb{F}[x]$, the congruence class $[a(x)]$ modulo $f(x)$ contains a unique representative $r(x)$ with deg($r(x)$)<deg($f(x)$) or $r(x) = 0$.*

Proposition 5.2. *Let $\mathbb{F}$ be a field, and let $f(x)$ be a nonzero polynomial in $\mathbb{F}[x]$. For any polynomials $a(x), b(x), c(x)$, and $d(x)$ in $\mathbb{F}[x]$, the following conditions hold:*

(a) *If $a(x) \equiv c(x) (\mathrm{mod}\, f(x))$ and $b(x) \equiv d(x) (\mathrm{mod}\, f(x))$, then*
$a(x) + b(x) \equiv c(x) + d(x) (\mathrm{mod}\, f(x))$ *and*
$a(x)b(x) \equiv c(x)d(x) (\mathrm{mod}\, f(x))$.

(b) *If gcd($f(x), a(x)$)=constant, then*
$a(x)b(x) \equiv a(x)c(x) (\mathrm{mod}\, f(x))$ *implies*
$b(x) \equiv c(x) (\mathrm{mod}\, f(x))$.

Proposition 5.3. *Let $\mathbb{F}$ be a field, and let $f(x)$ be a nonzero polynomial in $\mathbb{F}[x]$. For any $a(x) \in \mathbb{F}[x]$, the congruence class $[a(x)]$ has a multiplicative inverse in $\mathbb{F}[x]/(f(x))$ if and only if gcd($f(x), a(x)$)$\in \mathbb{F}$.*

Theorem 5.1. *Let $\mathbb{F}$ be a field and $f(x) \in \mathbb{F}[x]$ an irreducible polynomial with degree n over $\mathbb{F}$. Then, the set of equivalence classes $K = \mathbb{F}[x]/(f(x))$ is a field ($K = \mathbb{F}(x)$) with respect to addition and multiplication of polynomials modulo $f(x)$.*

Note that: with $(\ f(x)\ )$ or $\langle\ f(x)\ \rangle$ we denote the set of polynomials each of which has as a factor the element $f(x)$.
Proving that $\mathbb{F}(x)$ is a field can be done through a direct validation that all the elements except 0 has a multiplicative inverse. Indeed, given $a(x) \in \mathbb{F}(x)$, being $\gcd(f(x), a(x))$=`constant` then there exist two polynomials $\xi(x), \eta(x)$ such that $1 = \xi(x)f(x) + \eta(x)a(x) \Rightarrow a(x)^{-1} \equiv \eta(x) \bmod f(x)\ \forall\, a(x) \in \mathbb{F}(x)$

Proposition 5.4. *Let $\mathbb{F}$ be a field and $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{F}[x]$ an irreducible polynomial with degree n over $\mathbb{F}$. Polynomial $f(y)$ is reducible when it is considered as a polynomial with coefficients in $K = \mathbb{F}[x]/(f(x))$. Indeed, it has at least one root in K equal to the coset $x + < f(x) >$.*

Proof. Given
$f(y) = (< f(x) > +a_n)y^n + (< f(x) > +a_{n-1})y^{n-1} + ... + (< f(x) > +a_0) \in K[y]$.
We compute $f(< f(x) > +x)$.
It follows that:
$f(< f(x) > +x) = (< f(x) > +a_n)(< f(x) > +x)^n +$
$+(< f(x) > +a_{n-1})(< f(x) > +x)^{n-1} + \ldots + (< f(x) > +a_0) =$
$= (a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0) = f(x) =< 0 >$
where $< 0 >$ is the class equivalent to 0 in K.
Therefore, in K we have that

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0 \Leftrightarrow x^n = -a_n^{-1}(a_{n-1}x^{n-1} + \ldots + a_0)$$

□

Given $K = \mathbb{F}(x) = \mathbb{F}[x]/(f(x))$ we usually identify each equivalence class with its representative polynomial chosen as the one with smallest degree and unitary leading coefficient. Given two polynomials $a(x), b(x) \in \mathbb{F}(x) = \mathbb{F}[x]/(f(x))$ with $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_i \in \mathbb{F}$ irreducible in $\mathbb{F}$, the modular multiplication $a(x) \cdot b(x) \bmod f(x)$ can be computed considering the equality $x^n = -a_n^{-1}(a_{n-1}x^{n-1} + \ldots + a_0)$ and not applying the division algorithm.

Example 5.1. *Given $K = \mathbb{Z}_3(x) = \mathbb{Z}_3[x]/(f(x))$, $f(x) = x^2 + x + 1 \in \mathbb{Z}_3[x]$, if $a(x) = x + 1$, $b(x) = 2x + 1$, then*
$a(x) \cdot b(x) = 2x^2 + 3x + 1 = 2(-x-1) + 3x + 1 = 2(-x-1) + 0 + 1 = -2x - 2 + 1$
$a(x) \cdot b(x) = x + 2$

Given a field $K = \mathbb{F}(x) = \mathbb{F}[x]/(f(x))$, $f(x)$ irreducible in $\mathbb{F}$ with degree $m = \deg(f(x))$, the multiplicative finite subgroup $(\mathbb{F}(x)\backslash\{0\}, \cdot)$ has a number of elements equal to $n = |\mathbb{F}|^m - 1$ therefore, in order to compute a multiplicative inverse in $K = \mathbb{F}(x)$ we can employ either the Euclid's Algorithm or the relation $a(x)^{-1} = a(x)^{n-1} \in K$.

Example 5.2. *Compute the multiplicative inverse of the following elements $f(x), h(x)$ in $\mathbb{F}(x) = \mathbb{Z}_3[X]/ < x^2 - x - 1 >$, $n = |\mathbb{F}(x)| = 3^2 - 1 = 8$*

$$g(x) = x + 1 \qquad h(x) = 2x$$

$$\begin{aligned}(g(x))^{-1} &= (x+1)^{8-1} \, mod \, f(x) = (x+1)^{111_2} \, mod \, f(x) = \\ &= ((x+1)^2(x+1))^2(x+1) \, mod \, f(x) = \cdots = 2x + 2.\end{aligned}$$

$$\begin{aligned}(h(x))^{-1} &= (2x)^{8-1} \, mod \, f(x) = (2x)^{111_2} \, mod \, f(x) = \\ &= ((2x)^2(2x))^2(2x) \, mod \, f(x) = \cdots = 2x + 1.\end{aligned}$$

Analogously, being $f(x)$ irreducible in $\mathbb{F}$ the application of the Euclidean algorithm in the polynomial ring $\mathbb{F}[x]$ allows to write the following:

$$f(x) = x^2 - x - 1, \; g(x) = x + 1 \Rightarrow \; 1 = \gcd(f(x), g(x)) = f(x)\xi(x) + g(x)\eta(x)$$

Thus, the computation modulo $f(x)$ of both members of the last equality gives us:

$$g(x)^{-1} = \big(\eta(x) \bmod f(x)\big)$$

Inverse of $g(x) = x + 1$:

$$\begin{cases} \underline{u} \leftarrow (x^2 - x - 1, 1, 0); \\ \underline{v} \leftarrow (x + 1, 0, 1); \end{cases}$$

$$\begin{cases} q = \lfloor \frac{x^2-x-2}{x+1} \rfloor = x - 2,\ \underline{w} \leftarrow (x^2 - x - 1 - (x+1)(x-2), 1, -(x-2)); \\ \underline{u} \leftarrow (x + 1, 0, 1); \\ \underline{v} \leftarrow (1, 1, -x + 2); \end{cases}$$

$$\begin{cases} q = \lfloor \frac{x+1}{1} \rfloor = x + 1,\ \underline{w} \leftarrow (x + 1 - (x+1), 0 - (x+1), 1 - (-x+2)(x+1)); \\ \underline{u} \leftarrow (1, 1, 2x + 2); \\ \underline{v} \leftarrow (0, 2x + 2, x^2 - x - 1); \end{cases}$$

$$d(x) = 1;\ \xi(x) = 1;\ \eta(x) = 2x + 2 \Rightarrow (g(x))^{-1}\ mod\ f(x) = \mathbf{2x + 2}$$

Inverse of $h(x) = 2x$:

$$f(x) = x^2 - x - 1,\ h(x) = 2x \Rightarrow\ 1 = \gcd(f(x), g(x)) = f(x)\xi(x) + g(x)\eta(x)$$

$$\begin{cases} \underline{u} \leftarrow (x^2 - x - 1, 1, 0); \\ \underline{v} \leftarrow (2x, 0, 1); \end{cases}$$

$$\begin{cases} q = \lfloor \frac{x^2-x-1}{2x} \rfloor = 2x + 1,\ \underline{w} \leftarrow (-1, 1, x - 1); \\ \underline{u} \leftarrow (2x, 0, 1); \\ \underline{v} \leftarrow (-1, 1, x - 1); \end{cases}$$

$$\begin{cases} q = \lfloor \frac{2x}{-1} \rfloor = x,\ \underline{w} \leftarrow (0, 2x, 2x^2 + x + 1); \\ \underline{u} \leftarrow (-1, 1, x - 1); \\ \underline{v} \leftarrow (0, 2x, 2x^2 + x + 1); \end{cases}$$

$$d(x) = \xi(x)f(x) + \eta(x)h(x), \quad d(x) = -1;\ \xi(x) = 1;\ \eta(x) = x - 1 \Rightarrow$$
$$-1 = (1)f(x) + (x - 1)h(x) \Leftrightarrow$$
$$1 = (-1)f(x) + (2x + 1)h(x) \Rightarrow$$
$$\eta(x) = (h(x))^{-1}\ mod\ f(x) = \mathbf{2x + 1}\ mod\ f(x)$$